Grid Security Protocols and Infrastructure

Doug Engert, Ian Foster, Carl Kesselman, Steven Tuecke, Von Welch

Grid Characteristics

- The Grid is fundamentally about access to and coupling of resources, e.g. via
  - Desktop access to remote computers, mass storage systems, etc.
  - Collaborative design, analysis, visualization
  - Real-time, remote access to instruments
  - Massive computation through coupled supercomputers
  - Large parameter studies through the use of under-utilized resources

Why Grid Security is Hard

- The resources being used may be extremely valuable and the problems being solved extremely sensitive
- Resources are often located in distinct administrative domains
- The set of resources used by a single computation may be large, dynamic, and/or unpredictable
- International issues

Grid Security Requirements

- Each facility has own policies and procedures
  - Resource owners must maintain control
  - Inter-operate with local solutions (Kerberos)
  - Focus on inter-domain issues
- Applications require dynamic use of resources
  - Requires single sign-on and delegation
  - Need consistent infrastructure between sites
- International and inter-agency community
  - Focus on authentication, authorization, and accounting; privacy can raise export issues

the globus project
www.globus.org

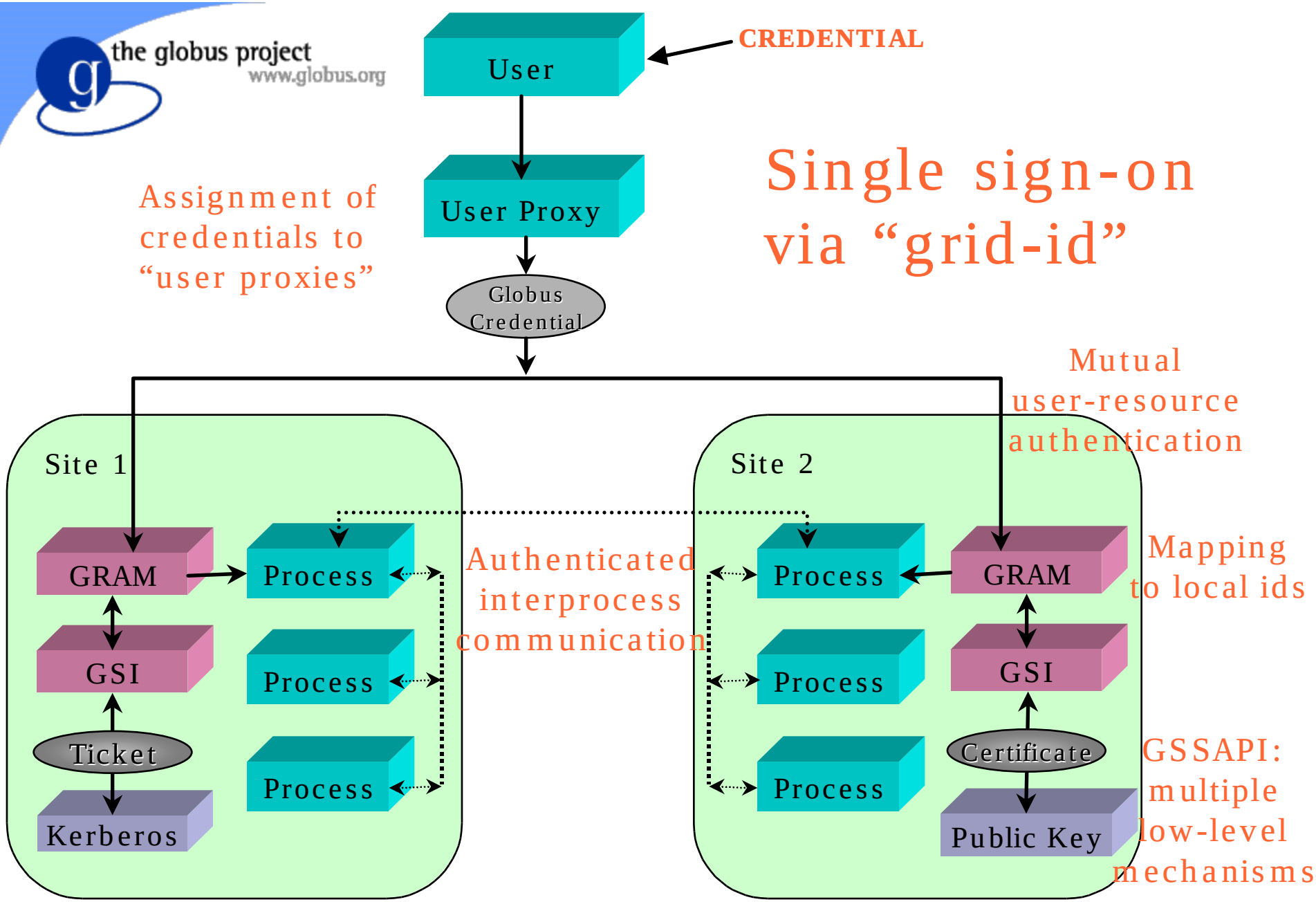
General Approach

- Define the Grid Security Protocols (GSP)
  - Integrate and extend existing protocols
  - Secure single sign-on, authentication, authorization, integrity, privacy
- Implement the Grid Security Infrastructure
  - Open source implementation of GSP
  - Client & server software development kits
  - PKI management tools
  - Interoperability tools: Kerberos, Portals
- GSP-enable wide variety of tools
  - FTP, SSH, Condor, Globus, SRB, MPI, etc.

the globus project
www.globus.org

Single sign-on via "grid-id"

Assignment of credentials to "user proxies"



What Grid Security Looks Like (Depends Who You Are ...)

User View

- Single sign-on (PKI)

  grid_proxy_init, MyProxy

2) Run apps: ftp, ssh, MPI, Condor, Portals, LDAP, ...

Resource Owner View

- Specify access control

  CA policy/gridmap files, GAA

2) Auditing, accounting, etc.

  TBD

Developer View

Verify identity; message integrity & privacy; delegation

Direct calls to various GSS-API calls

Or: GlobusIO functions for secure TCP, etc., etc.

Low-level details

1) A combination of existing protocols

X.509, TLS (SSL), CRL, ...

2) With a number of interesting extensions

GSS-API/SSL binding, user proxies, delegation, gateways

Interoperability: MyProxy

- Credential cache
  - User deposits proxy into cache
  - Associates a name and password, which can later be used to retrieve a proxy from cache
- Various uses:
  - Portals: Allows user to delegate to web portal server, even when logging from anywhere (I.e., user's credentials not available)
  - Novice user credential management: Rather than having user manage long term credentials, can instead keep them in MyProxy

Interoperability: K5cert

- Kerberos site can create an automatic, online certificate authority
  - User logs into Kerberos realms as normal
  - User runs K5cert client to generate a proxy
    - Client uses Kerberos ticket to authenticate with K5cert
    - K5cert creates X.509 proxy, signed by K5cert online CA
- Kerberos user can easily acquire a short-term PKI credential
  - But requires new CA, which resources must trust for users to gain access
  - Could combine K5cert and MyProxy?

GSI Applications Include ...

- Globus toolkit uses GSI for authentication in all resource management, data management, etc., functions
- Many Grid tools, directly or indirectly, e.g.
  - Condor, SRB, MPICH-G2, etc.
- Commercial and open source tools, e.g.
  - ssh and ftp
  - SecureCRT (Win32 ssh client)
- And credentials can also be used for
  - Web access, LDAP server access

GSP/GSI Adoption

- Adopting GSI = CA + libraries + tools
- Rollouts are currently underway at:
  - NCSA Alliance, NPACI
  - NASA Information Power Grid
  - DOE Science Grid (started)
- And, in addition
  - GrADS testbed, European Data Grid, GriPhyN, NEESgrid, others
- Significant commercial interest
  - Standardization & commercial use

the globus project
www.globus.org

Future Directions (1)

- Authentication
  - Investigate techniques to further reduce exposure from compromised session credentials
    - Note: Same issue exists in Kerberos cross-realm setups
  - Smartcards
  - Group authentication methods
- Authorization
  - IETF Draft GAA-API implementation completed
  - Policy based resource management research
  - Applications in Data Grid context

the globus project
www.globus.org

Future Directions (2)

- Delegation: restricted proxies
  - Experiments with ClassAds
- Accounting & Auditing
  - Integration with NCSA account management
  - Tools for distributed accounting & auditing
- Dynamic accounts
  - On-demand allocation of accounts, hence avoiding a need for pre-existing accounts
- IDUP-GSS-API Binding to GSP
  - Independent Data Unit Protection

Summary

- GSP and GSI successfully address wide variety of Grid security issues
- Broad acceptance, deployment, integration with tools
- For more information:
  - www.globus.org/research/papers.html
  - “A Security Architecture for Computational Grids”
  - “Design and Deployment of a National-Scale Authentication Infrastructure”